UNITED STATES DISTRCIT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

BARRY COTTON, GARY LAKE, individually and on behalf of all others similarly situated, Plaintiffs, v. JERICO PICTURES, INC. d/b/a NATIONAL PUBLIC DATA Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Barry Cotton and Gary Lake ("Plaintiffs"), individually and on behalf of others similarly situated (the "Class" or "Class members"), hereby bring this class action complaint against Defendant, Jerico Pictures, Inc. d/b/a National Public Data ("Defendant"). Plaintiffs allege as follows upon personal knowledge as to their own acts and experiences, and upon the investigation of their attorneys as to all other matters.

INTRODUCTION

1. This is a data breach class action on behalf of individuals whose personally identifying information ("PII) was stolen by cybercriminals as part of a major cyber-attack on Defendant's systems. It was reported that on or about April 8, 2024, there was unauthorized access to Plaintiffs' and many other individuals' PII and that the information was put up for sale on the

dark web (the "Data Breach").[1] Information compromised in the breach included full names, dates of birth, addresses, Social Security number (SSN), family history, and other sensitive and private data.[2]

2. Defendant is a public records data provider specializing in background checks and fraud prevention.[3]

3. As a condition of receiving services, consumers of Defendant pay monies to Defendant to receive access to its massive database, which upon information and belief is comprised of individuals' PII. Additionally, and upon information and belief, consumers may also provide sensitive and personal information to Defendant such as PII to populate Defendant's database.

4. By taking possession and control of sensitive information such as PII, Defendant assumed a duty to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals' PII from unauthorized disclosure.

5. Defendant also has a duty to adequately safeguard individuals' sensitive and private information under industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act ("FTC Act"), and other relevant laws and regulations.

6. Defendant breached its duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect individuals' PII from unauthorized access and disclosure.

7. On June 1, 2024, it was reported by VX-Underground that Defendant's database of

---

[1] https://x.com/vxunderground/status/1797047998481854512?lang=en (last visited July 29, 2024).
[2] *Id.*
[3] https://nationalpublicdata.com/

2.9 billion records containing individuals' personal information, including their social security numbers, was posted online for sale for $3.5 million by the cybercriminal group known as "USDoD, who had improperly accessed the data on Defendant's network back in April 2024."[4]

8. The report noted that VX-Underground was provided access to the database and it was able to confirm the validity of the data.[5]

9. Defendant has not publicly addressed the Data Breach, nor provided any notice to affected individuals. It is presently unknown if an official investigation was ever opened by Defendant into the event.

10. However, on or about July 29, 2024, Plaintiffs and Class members received notice that their personal data, including their PII and social security numbers, was compromised in the Data Breach and found on the dark web. Plaintiffs and Class members received these notices from various credit and identity protection monitoring services.

11. Defendant has offered no assurance that the sensitive and private information that was accessed in the Data Breach has been recovered or destroyed.

12. The exposure of a person's PII through a data breach substantially increases that person's risk of identity theft, fraud, and similar forms of criminal mischief, potentially for the rest of their lives. Mitigation of such risk requires individuals to expend a significant amount of time and money to closely monitor their credit, financial accounts and email accounts. Mitigation of the risk of misuse of their sensitive and private information may not even be possible.

13. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII was accessed and

[4] *Supra* n.1.
[5] *Id.*

disclosed. Plaintiffs and Class members are now at a substantially increased risk of experiencing misuse of their PII in the coming years. This action seeks to remedy these failings and their consequences.

14. The injury to Plaintiffs and Class members is compounded by the fact that Defendant has yet to address the Data Breach and notify the victims of its occurrence. Defendant's failure to timely notify the victims of the Data Breach meant that Plaintiffs and Class members were unable to take premature measures to prevent or mitigate the resulting harm.

15. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was stolen in the Data Breach. Plaintiffs assert claims for negligence, breach of fiduciary duty, breach of implied contract, unjust enrichment, and invasion of privacy, and seek declaratory relief, injunctive relief, monetary damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiffs

16. Plaintiff Barry Cotton is an adult residing in Austin, Texas who has received notice from both a credit monitoring and identity protection company that his PII, including his social security number was found on the dark web as a result of the Data Breach.

17. Plaintiff Gary Lake is an adult residing in Cumberland, Rhode Island who has received notice from a credit monitoring company that his PII, including his social security number was found on the dark web as a result of the Data Breach.

Defendant

18. Defendant Jericho Pictures, Inc. is a Florida corporation and independent film company that owns the fictitious name National Public Data.

19. National Public Data is operated and controlled by Defendant Jericho Pictures, Inc.,

and is a public records data provider specializing in background checks and fraud prevention with a principal place of business located at 1440 Coral Ridge Dr. Suite 236, Coral Springs, FL 33071.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million dollars, exclusive of interest and costs, and is a class action in which some members of the class are citizens of states different than Defendant. See 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

21. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District, regularly conducts business in this District, and the acts and omissions giving rise to Plaintiffs' claims emanated from within this District.

22. Venue is proper under 18 U.S.C. § 1391(b) because Defendant maintains its principal place of business in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant Collects and Stores PII

23. Defendant conducts business under the name National Public Data and is a public records data provider specializing in background checks and fraud prevention. Defendant advertises that its services are used by private investigators, background check websites, data resellers, mobile apps, applications, and more.[6]

24. Defendant guarantees freshness and quality of data at low cost, and represents that its data hub is updated regularly.[7]

---

[6] https://nationalpublicdata.com/index.html.
[7] https://nationalpublicdata.com/about-us.html.

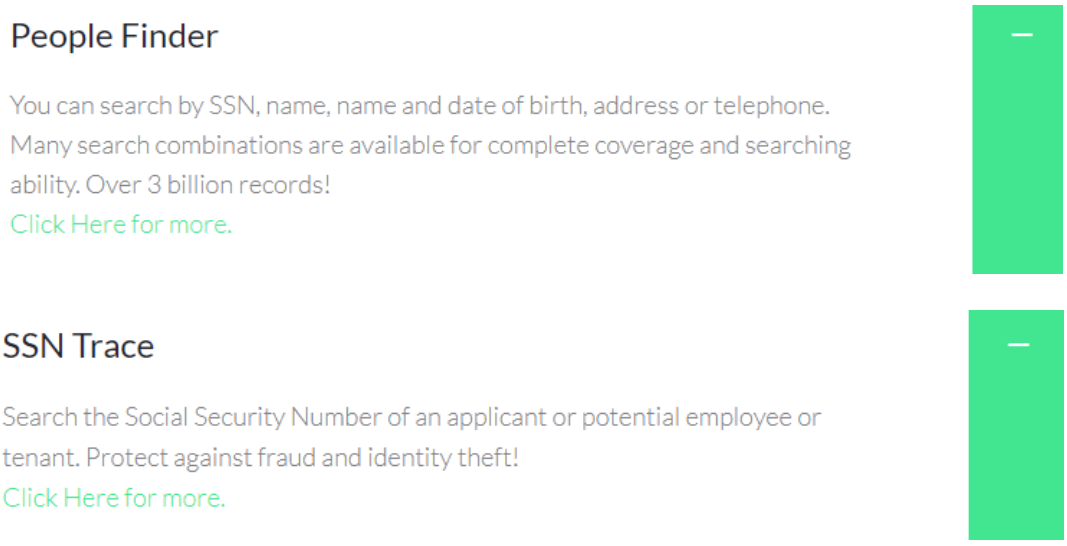
25. Defendant utilizes XML API gateway to instantly deliver data to consumers.[8]

26. Upon information and belief, Defendant engages in the practice of assembling or evaluating sensitive information of individuals such as PII for the purpose of furnishing that information to consumers.

27. Additionally, upon information and belief, Defendant obtains personal and sensitive information from individuals, including their social security numbers to complete assemble its database of records, complete background checks and to otherwise carry out its business.

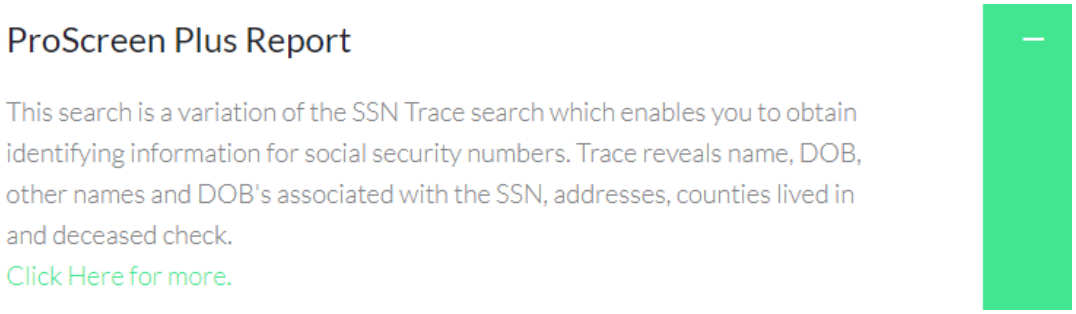
28. Defendant collects and maintains such information on its servers.

29. For example, in or about January 2024, Defendant's website contained the following representations about the databases it hosts[9]:



[8] *Supra* n.5.

[9] https://web.archive.org/web/20240117042155/http://www.nationalpublicdata.com/databases.html (Jan. 17, 2024) (last visited July 29, 2024).



30. In or about January 2024, Defendant also advertised the availability of other databases such as criminal records, sex offender records, USA Consumer Data, cell phone/ unlisted number search, marriage and divorce, email address search, SSDI Death Index, voter registration, people at work, physician background check, FAA Pilots and Planes, USA Business Profiles, Canadian Business Profiles, White and Yellow Pages, Merchant vessels, vehicle ownership, Canadian people finder, national Medicare sanctions, bankruptcy search, OFAC/SDN/terrorist search.[10]

31. Defendant no longer advertises the specific databases that it hosts. Instead, Defendant encourages visitors to contact a representative for further information.[11]

32. On information and belief, the type of information that Defendant maintains includes, *inter alia*: full names, addresses, dates of birth, Social Security number ("SSN"), and any other information necessary to maintain its database and otherwise carry out its business.

33. Due to the highly sensitive nature of the information Defendant collects and maintains, Defendant is obligated provide confidentiality and adequate security for individuals information in compliance with statutory privacy requirements and industry standards.

34. Upon information and belief, Plaintiffs and Class members may have provided their PII, including their social security numbers to Defendant.

---

[10] *Id.*

[11] https://nationalpublicdata.com/contacts.html

35. Plaintiffs and Class members received notice beginning on or about July 29, 2024, that their information which was in Defendant's possession was stolen in the Data Breach. The notice came not from Defendant, but rather various credit monitoring and identity monitoring services.

36. The notices received by Plaintiffs and Class members specifically mention that their data was compromised in the Data Breach.

37. Plaintiffs and Class members are entitled to protections to keep their sensitive PII, including their social security numbers, confidential and secured, to use such information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew that Criminals Target Valuable PII and Failed to Take Action to Prevent Theft

38. At all relevant times, Defendant knew it was storing sensitive PII and that, as a result, Defendant's systems would be attractive for cybercriminals.

39. Defendant also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

40. The risks are not theoretical. The prevalence of data breaches has increased dramatically over the years: "The number of reported data breaches in the U.S. rose to a record 3,205 in 2023, up 78% from 2022 and 72% from the previous high-water mark in 2021, according to the nonprofit Identity Theft Resource Center."[12]

41. In recent years, numerous high-profile breaches have occurred including breaches

[12] Stuart Madnick, *If Companies Are So Focused on Cybersecurity, Why Are Data Breaches Still Rising?*, THE WALL STREET JOURNAL (Mar. 15, 2024), https://www.wsj.com/tech/cybersecurity/why-are-cybersecurity-data-breaches-still-rising-2f08866c (last visited July 29, 2024).

involving MoveIt, First American Financial Corp., JP Morgan Chase & Co., and Equifax.

42. In tandem with the increase in data breaches, the rate of identity theft has increased. Since 2019, identity theft reports have increased $68.3%. In the second quarter of 2023, roughly 277,620 ID theft reports were submitted to the Federal Tarde Commission, which was a substantial increase from the 164,982 reported in the same quarter in 2019.[13]

43. Every state has experienced an increase in identity theft over 11% per 100,000 residents since 2019.[14]

44. PII has considerable value to hackers. Hackers sell stolen data on the black market through the "proliferation of open and anonymous cybercrime forums on the Dark Web that server as a bustling marketplace for such commerce."[15]

45. The breadth of data that can be bought and sold leaves Defendant's consumers especially vulnerable to identity theft, tax fraud, credit and bank fraud.

46. Consumers also place a high value on the privacy of their data. Studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[16]

47. Recently, more consumers are exercising their Data Subject Access Rights and

---

[13] Julie Ryan Evans, *93 of 100 Largest US Metros and All States Hae Seen Increase in ID Theft Reports Since 2019*, LENDINGTREE (Nov. 6, 2023), https://www.lendingtree.com/insurance/id-theft-study/#:~:text=Identity%20theft%20reports%20have%20increased,the%20same%20quarter%20in%202019 (last visited July 29, 2024).

[14] *Id.*

[15] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited July 29, 2024).

[16] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), available for download at: https://www.jstor.org/stable/23015560?seq=1.

leaving providers over their data practices and policies.[17]

48. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

49. Defendant certainly knew and understood that unprotected or exposed PII in its custody is highly valuable and sought after by nefarious criminals seeking to illegally monetize that PII through unauthorized access.

50. Armed with this knowledge, Defendant breached its duties by failing to implement and maintain reasonable security measures to protect Plaintiffs' and Class members' PII from being stolen.

The Data Breach

51. On June 1, 2024, it was reported by VX-Underground that Defendant's database of 2.9 billion records containing individuals' personal information, including their social security numbers, was posted online for sale for $3.5 million by the cybercriminal group known as "USDoD, who had improperly accessed the data on Defendant's network back in April 2024.[18]

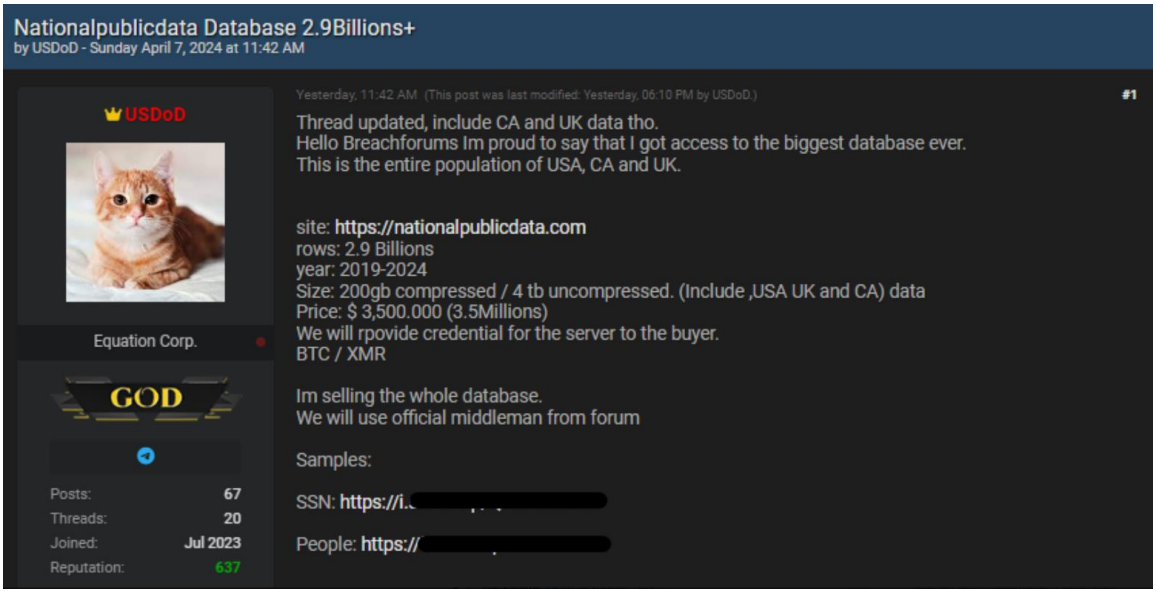
52. Indeed, the technology security company HackManac posted on its X Account on April 8, 2024, that cybercriminal group USDoD was threatening to sell a 4 TB database containing 2.9 billion records that it stole from National Public Data's network for $3.5 million.[19] HackManac included in its post a screenshot of USDoD's threat as posted on a dark web forum:

---

[17] CISCO, *Cisco 2023 Consumer Privacy Survey* (April 2023), available at https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html?CCID=cc000742

[18] *Supra* n.1.

[19] https://x.com/H4ckManac/status/1777246310782902686/photo/1 (last visited July 29, 2024).



53. The validity of the data was confirmed by XV-Underground.[20]

54. Defendant has not publicly acknowledged the Data Breach, nor has it provided any indication that it occurred and that an investigation is ongoing. Defendant has not issued individual notifications to affected individuals.

55. However, Plaintiffs and Class members received notice from various credit monitoring and identity monitoring services beginning July 29, 2024, that their PII including their social security numbers was accessed in the Data Breach and thereafter found on the dark web.

56. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as an entity that collects, creates, and maintains PII on its computer network and/or systems.

57. Plaintiffs' and Class members' PII was compromised and acquired in the Data Breach.

58. Due to this targeted cyberattack, data thieves were able to gain access to and obtain data from the Defendant that included the PII of Plaintiffs and Class members.

59. As evidenced by the Data Breach's occurrence, the PII contained on Defendant's

[20] *Supra* n.1.

systems was not encrypted. Had it been, the data thieves would have stolen only unintelligible data.

60. Plaintiffs and Class members now live with their PII exposed in cyberspace and available to people willing to purchase and use the information for any number of improper purposes and crimes.

61. Plaintiffs and Class members now face constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class members are incurring and will continue to incur such damages, in addition to any fraudulent use of their PII.

Plaintiff Barry Cotton's Experience in the Data Breach

62. On or about July 29, 2024, Plaintiff Barry Cotton received notice from both Experian, a credit monitoring company, and LifeLock, an identity theft monitoring company, that his personal information, including his social security number, was found on the dark web.

63. The notices to Plaintiff specifically mentioned that his personal information was compromised in Defendant's Data Breach.

64. Plaintiff's PII was exposed and accessed in the Data Breach.

65. As a result, Plaintiff has had to spend time and resources monitoring his credit report and financial accounts for fraudulent activity.

66. Plaintiff is careful about sharing his private information. Plaintiff stores any documents containing private information in a safe and secure location. He never knowingly transmitted unencrypted private information over the internet or any other unsecured medium. Plaintiff would not have entrusted his private information with Defendant had he known of Defendant's failure to implement and maintain data security measures.

67. Plaintiff is now at a substantial risk of identity theft and will spend future time and

resources to monitor his accounts and mitigate the risk of identity theft and/or other types of fraud.

Plaintiff Gary Lake's Experience in the Data Breach

68. On or about July 29, 2024, Plaintiff Gary Lake received notice from MyIDcare, a credit and identity theft monitoring company, that his personal information, including his social security number, was found on the dark web.

69. The notice to Plaintiff specifically mentioned that his personal information was compromised in Defendant's Data Breach.

70. Plaintiff's PII was exposed and accessed in the Data Breach.

71. As a result, Plaintiff has had to spend time and resources monitoring his credit report and financial accounts for fraudulent activity.

72. Plaintiff is careful about sharing his private information. Plaintiff stores any documents containing private information in a safe and secure location. He never knowingly transmitted unencrypted private information over the internet or any other unsecured medium. Plaintiff would not have entrusted his private information with Defendant had he known of Defendant's failure to implement and maintain data security measures.

73. Plaintiff is now at a substantial risk of identity theft and will spend future time and resources to monitor his accounts and mitigate the risk of identity theft and/or other types of fraud.

Defendant Failed to Comply with the FTCA and FTC Guidelines

74. The Federal Trade Commission Act ("FTCA") prohibits Defendant from engaging in "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45.

75. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which reflect the importance of implementing reasonable data security practices.

76. The FTC's publication, Protecting Personal Information, established cyber-security

guidelines for businesses. The guidelines provide that businesses should take action to protect the personal information that they collect; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems.[21]

77. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[22]

78. The FTC further recommends that businesses not maintain private information longer than is needed for authorization of a transaction; limit access to sensitive information; require complex passwords be used on networks; use industry-tested methods for security monitor for suspicious activity on the networks; and verify that third-party service providers have implemented reasonable security measures.

79. The FTC has the authority to bring enforcement actions against businesses for failing to protect PII adequately and reasonably under Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

80. The orders that result from enforcement actions further clarify the measures businesses must take to meet their data security obligations.

81. Defendant failed to properly implement basic data security practices.

82. Defendant was at all relevant times fully aware of its obligations to protect

---

[21] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[22] *Id.*

individuals' PII, and of the significant consequences that would result from its failure to do so.

83. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

84. Consequently, cybercriminals circumvented Defendant's lax security measures, resulting in the Data Breach and causing injury to Plaintiffs and Class members.

Defendant Failed to Comply with Industry Standards

85. Entities like Defendant are particularly vulnerable to cyberattacks because of the sensitive nature of the information that they collect and maintain.

86. Due to this vulnerability, there are industry best practices that should be implemented by entities like Defendant.

87. These practices include but are not limited to: Educating and training employees about the risks of cyberattacks, strong passwords, multi-layer security such as firewalls, anti-virus and malware software, encryption, multi-factor authentication, backup data, limitation of employees with access to sensitive data, setting up network firewalls, switches and routers, monitoring and limiting the network ports, and monitoring and limited access to physical security systems.

88. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

89. The Defendant's failure to implement the industry standards described herein resulted in the Data Breach and caused injury to Plaintiffs and Class members.

Common Damages Sustained by Plaintiffs and Class Members

90. For the reasons mentioned above, Plaintiffs and all other Class members have suffered injury and damages directly attributable to Defendant's failure to implement and maintain adequate security measures, including, but not limited to: (i) fraudulent credit card applications attempted in their name (ii) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) invasion of their privacy; (v) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

CLASS ALLEGATIONS

91. Plaintiffs bring this class action individually and on behalf of all persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

92. Plaintiffs seek certification of a Class as defined below and subject to further amendment:

> **Nationwide Class**
>
> All individuals in the United States whose PII was compromised in the Data Breach (the "Class").
>
> **State Subclass**
>
> All individuals residing in Ohio whose PII was compromised in the Data Breach (the "Ohio Subclass").

93. Excluded from the Class is Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of

said judge(s).

94. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

95. Numerosity. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. It was reported that approximately 2.9 billion records was exposed in the Data Breach. The number of individuals and contact information of those individuals are available from Defendant's business records.

96. Commonality. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

- Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII from unauthorized access and disclosure;
- Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII;
- Whether Defendant breached its duties to protect Plaintiffs' and Class members' PII;
- Whether defendant breached its fiduciary duty to Plaintiffs and Class members;
- When Defendant learned of the Data Breach;
- Whether Defendant knew or should have known that its data security systems and monitoring procedures were deficient;
- Whether hackers obtained Plaintiffs' and Class members data in the Data Breach;
- Whether an implied contract existed between Plaintiffs, Class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Plaintiffs' and Class members' PII from unauthorized access and disclosure;

- Whether Defendant was unjustly enriched;
- Whether Defendant invaded Plaintiffs' and Class members' privacy by causing the Data Breach;
- Whether Plaintiffs and Class members are entitled to injunctive relief and identity theft protection to redress the imminent harm they face due to the Data Breach; and
- Whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

97. Typicality. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

98. Adequacy of Representation. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or in conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

99. Superiority. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress from Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and

increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

100. All members of the proposed Class are readily ascertainable. Defendant has access to the names, addresses, and/or email addresses of Class members affected by the Data Breach.

101. Finally, class certification is appropriate under Fed. R. Civ. P. 23(b). Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

CAUSES OF ACTION
COUNT I
NEGLIGENCE
(Plaintiffs, individually and on behalf of the Nationwide Class, or alternatively, the State Subclass)

102. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

103. Defendant requires that its consumers, including Plaintiffs and Class members, submit private information such as PII in the course of providing its services.

104. Defendant collected, acquired, and stored Plaintiffs' and Class members' private information on its servers.

105. Plaintiffs and Class members entrusted Defendant with their private information and had the understanding that Defendant would safeguard their information.

106. Defendant had knowledge of the sensitivity of Plaintiffs and Class members' private information, and the consequences that would result from the unauthorized disclosure of

such information. Defendant knew that entities such as them were the target of cyber-attacks in the past, and that Plaintiffs and Class members were the foreseeable and probable victims of any inadequate data security procedures.

107. It was therefore reasonably foreseeable that the failure to implement adequate data security procedures would result in injuries to the Plaintiffs and Class members.

108. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their private information in its possession, custody, or control from the unauthorized disclosure of such information.

109. Defendant's duty to exercise reasonable care arises from several sources, including but not limited to common law, the FTCA, and industry standards.

110. Defendant breached its duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiffs' and Class members' PII.

111. It has been reported that the PII of Plaintiffs and Class members was disclosed to unauthorized third persons as a result of the Data Breach. Further, Plaintiffs and Class members have received notice from credit and identity monitoring services that their PII was found on the dark web because of the Data Beach.

112. Defendant's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members caused their PII to be compromised in the Data Breach.

113. Plaintiffs and Class members were in no position to protect their PII themselves.

114. But for Defendant's breach of the duties described herein, Plaintiffs and Class

members' PII would not have been compromised.

115. There is a causal relationship between Defendant's failure to implement, control, direct, oversee, manage, monitor, and audit adequate data security procedures to protect the PII of individuals and the harm suffered by Plaintiffs and Class members.

116. As a direct and proximate result of Defendant's conduct described above, it directly and proximately caused the Data Breach, and Plaintiffs and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII; (iv) breach of the confidentiality of their PII; (v) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

117. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

118. Plaintiffs and Class members are entitled to damages incurred as a result of the Data Breach.

119. Defendant's negligent conduct is ongoing, in that it still holds Plaintiffs' and Class members PII in an unsafe and insecure manner.

120. Plaintiffs and Class members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to

Class members.

COUNT II
BREACH OF FIDUCIARY DUTY
(Plaintiffs, individually and on behalf of the Nationwide Class, or alternatively, the State Subclass)

121. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

122. Plaintiffs and Class members gave Defendant their PII in confidence, believing that Defendant would protect that information. Plaintiffs and Class members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiffs' and Class members' PII created a fiduciary relationship between Defendant and Plaintiffs and Class members. In light of this relationship, Defendant must act primarily for the benefit of its consumers, which includes safeguarding and protecting Plaintiffs' and Class members' PII.

123. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class members' PII, failing to comply with Section 5 of the FTCA and industry standards, and otherwise failing to safeguard Plaintiffs' and Class members' PII that it collected.

124. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII; (iv) breach of the confidentiality of their PII; (v) deprivation of the value of their PII, for which there is a well-established national and international market;

and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

COUNT III
BREACH OF IMPLIED CONTRACT
(Plaintiffs, individually and on behalf of the Nationwide Class, or alternatively, the State Subclass)

125. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

126. In connection with receiving services from Defendant, Plaintiffs and all other Class members entered into implied contracts with Defendant or were intended third-party beneficiaries of contracts between Defendant and others.

127. Pursuant to these implied contracts, money was paid to Defendant, whether directly from Plaintiffs and Class members or indirectly, and Defendant stored the PII of Plaintiff and Class members on its network. In exchange, Defendant impliedly agreed to, among other things, take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and protect Plaintiffs' and Class members' PII in compliance with federal and state laws and regulations and industry standards.

128. The protection of PII was a material term of the implied contracts that were either between Plaintiffs and Class members, on the one hand, and Defendant, on the other hand or were between third parties and Defendant to which Plaintiffs and Class members were intended third party beneficiaries.

129. Plaintiffs and Class members or the third parties fulfilled their obligations under the contracts.

130. Defendant breached its obligations by failing to implement and maintain reasonable data security measures to protect and secure the PII and in failing to implement and maintain

security protocols and procedures to protect Plaintiffs' and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

131. Defendant's breach of its obligations of its implied contracts directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

132. Plaintiffs and all other Class members were damaged by Defendant's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) they suffered actual identity theft; (iv) their PII was improperly disclosed to unauthorized individuals; (v) the confidentiality of their PII has been breached; (vi) they were deprived of the value of their PII, for which there is a well-established national and international market; and/or (vii) they lost time and money to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

COUNT IV
UNJUST ENRICHMENT
(Plaintiffs, individually and on behalf of the Nationwide Class, or alternatively, the State Subclass)

133. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

134. This count is pleaded in the alternative to Plaintiffs' breach of implied contract claim (Count III)

135. Plaintiffs and Class members have an interest, both equitable and legal, in the private information about them that was collected, secured, and maintained by Defendant and that was ultimately compromised in the Data Breach.

136. A financial benefit was conferred upon Defendant when Plaintiffs and Class members provided payments to Defendant which contained their PII, including their social security numbers. Defendant's business model would not exist save for the need to ensure the security of Plaintiffs' and class members' private information.

137. The relationship between Defendant, Plaintiffs and Class members is not attenuated, as Plaintiffs and Class members had a reasonable expectation that the security of their information would be maintained when they provided their information to Defendant, or when Defendant otherwise took control of their information. Plaintiffs and Class members were induced to provide their information in reliance on the fact that Defendant's data security measures were adequate.

138. Upon information and belief, this financial benefit was, in part, conferred when portions of Plaintiffs and Class members' information were used by Defendant to obtain payments from other consumers for access to Defendant's database of personal information containing Plaintiffs' and Class member's PII, including their social security numbers.

139. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class members by acquiring and/or collecting their private information as a necessary part of obtaining Defendant's services. Defendant appreciated and benefitted from the receipt of Plaintiffs' and Class members' private information in that they used the private information and profited from the transactions in furtherance of its business.

140. Defendant also understood and appreciated that the PII pertaining to Plaintiffs and Class members was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

141. Defendant acquired Plaintiffs' and Class members' private information through

inequitable means in that it failed to disclose the inadequate data security procedures previously alleged herein.

142. As a result of Defendant's conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

143. Defendant should not be permitted to retain the payments which include information belonging to Plaintiffs and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class members paid for and that were otherwise mandated by federal and state law and industry standards.

144. Defendant unjustly enriched itself by using payments containing private information provided by Plaintiffs and Class members to further its business.

145. Notably, Defendant chose not to use any payments received to enhance their data security procedures.

146. Under principles of equity and good conscience, Defendant should not be permitted to retain the payments wrongfully obtained from Plaintiffs and Class members, and be compelled to provide for the benefit of Plaintiffs and Class members, all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
INVASION OF PRIVACY
(Plaintiffs, individually and on behalf of the Nationwide Class, or alternatively, the State Subclass)

147. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

148. As a condition of receiving services from Defendant, Plaintiffs and Class members were required to provide Defendant with their PII, including their social security numbers.

149. Defendant was under a legal duty to keep Plaintiffs' and Class members' PII safe from unauthorized disclosure.

150. Defendant invaded Plaintiffs' and Class members' privacy by failing to adequately safeguard their PII, thereby causing the Data Breach which resulted in the unauthorized access to Plaintiffs' and Class members' sensitive PII.

151. The invasion of privacy was public in nature, as the information was stolen by cybercriminals who thereafter converted Plaintiffs' and Class members' PII into a downloadable format and posted it on the web for others to purchase and use.

152. The intrusion was offensive to Plaintiffs and Class members, and to a reasonable person in that sensitive PII was accessed by unauthorized parties without Plaintiffs' and Class members' consent, and made public on the internet, increasing the risk of identity theft and other fraud.

153. The intrusion was into a place or thing which was private and is entitled to be private since Plaintiffs and Class members provided their PII to Defendant privately with the expectation that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

154. Due to the private nature of PII, it is not information that is of legitimate concern of the public.

155. Defendant intentionally caused Plaintiffs' and Class member's PII to be accessed by and unauthorized third party by willfully failing to enact adequate safeguards to protect their PII, despite knowing the risks faced by Plaintiffs and Class members in the event of an unauthorized disclosure.

156. As a direct and proximate result of Defendant's actions, Plaintiffs' and Class

members' PII was accessed by an unauthorized third party and shared on the internet.

157. Defendant's wrongful conduct will continue to cause Plaintiffs and Class members great harm since the PII maintained by Defendant was stolen and published on the dark web. Plaintiffs and Class members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiffs and Class members, and Defendant may freely treat Plaintiffs' and Class members' PII with inadequate safeguards.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representative, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: August 2, 2024

Respectfully submitted,

By: __/s/ John A. Yanchunis _____

John A. Yanchunis
JYanchunis@forthepeople.com
Antonio Arzola
ararzola@forthepeople.com
Ross Berlin
Ross.berlin@forthepeople.com
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, FL 33602
T: (813) 223-5505
F: (813) 223-5402

Steven A. Schwartz*
steveschwartz@chimicles.com
Beena M. McDonald*
bmm@chimicles.com
Alex M. Kashurba*
amk@chimicles.com
Marissa N. Pembroke*
mnp@chimicles.com
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500

**pro hac vice* to be submitted

Counsel for Plaintiff and the Proposed Class